A F-

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:	) Date: December 6, 2005
Ronald P. Sansone	) Attorney Docket No.: F-435
Serial No.: 10/015,469	) Customer No.: 00919
Filed: December 12, 2001	) Group Art Unit: 3621
Confirmation No.: 4625	) Examiner: Behrang Badii

Title: A SYSTEM FOR A RECIPIENT TO DETERMINE WHETHER OR NOT THEY RECEIVED NON-LIFE-HARMING MATERIALS

TRANSMITTAL OF APPEAL BRIEF (PATENT APPLICATION 37 CFR 1.192)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Transmitted herewith in **triplicate** is the **APPEAL BRIEF** in the above-identified

patent application with respect to the Notice of Appeal filed on October 7, 2005.

Pursuant to 37 CFR 1.17(c), the fee for filing the Appeal Brief is $500.00

Please charge Deposit Account No. **16-1885** in the amount of $500.00 to cover the

above fees.

The Commissioner is hereby authorized to charge any additional fees which may be

required to Deposit Account No. **16-1885**.

{10044024.1 }

A duplicate copy of this transmittal is enclosed for use in charging the Deposit Account.

<div align="right">

Respectfully submitted,

Ronald Reichman
Reg. No. 26,796
Attorney of Record
Telephone (203) 924-3854

</div>

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on December 5, 2005
Date of Deposit

Signature

Amy Harvey
Name of Person Certifying

{10044024.1 }

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:	) Attorney Docket No.: F-435
Ronald P. Sansone	) Group Art Unit: 3621
Serial No.: 10/015,469	) Examiner: Behrang Badii
Filed: December 12, 2001	) Date: December 6, 2005
Confirmation No.: 4625	) Customer No.: 00919

Title: **A SYSTEM FOR A RECIPIENT TO DETERMINE WHETHER OR NOT THEY RECEIVED NON-LIFE -HARMING MATERIALS**

APPELLANT'S BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This brief is in furtherance of the Notice of Appeal filed in this case on October 7, 2005.

This Brief is transmitted in triplicate.

TABLE OF CONTENTS

This brief contains these items under the following headings and in the order set forth below:

I   REAL PARTY IN INTEREST

Pitney Bowes Inc. is the real party in interest.

II   RELATED APPEALS AND INTERFERENCES

a) U.S. Patent Application Serial No. 10/015,464 entitled "Method And System For Accepting Non-Harming Mail At A Home Or Office" is presently on appeal to the Board Of Appeals.

b) U.S. Patent Application Serial No. 10/015,309 entitled "System For Receiving Non-Harming Mail At A Receptacle" is presently on appeal to the Board Of Appeals.

III   STATUS OF CLAIMS

a) Claims 1 - 18 are in the application.

b) Claims 1 - 18 are rejected.

c) Claims 1 - 18 are on appeal.

IV   STATUS OF AMENDMENTS

An amendment subsequent to the July 12, 2005, Final Rejection was filed on August 26, 2005. This amendment was not entered.

V   SUMMARY OF CLAIMED SUBJECT MATTER

A.   Background

The prior art does not provide a system that stores unique information that is affixed to mail and the identities of mailers; which has a scanner at a receptacle that reads the unique information before mail is permitted to enter the interior of

the receptacle; and, communicating to the recipient information stored in the data center about the mail.

People have used the United States Postal Service (USPS) and other courier services, e.g., Federal Express®, Airborne®, United Parcel Service,® DHL®, etc., hereinafter called "carriers", to deliver materials to recipients to whom the sender does not want to deliver personally. Unfortunately, sometimes the delivered materials may be illegal and/or hazardous to the health of the recipient and to the party who is delivering the goods, e.g., life-harming. Examples of life-harming materials are explosives; gun powder; blasting material; bomb; detonators; smokeless powder; radioactive materials; ammunition; atomic weapons; chemical compounds or any mechanical mixture containing any oxidizing and combustible units, or other ingredients in such proportions, quantities, or packing that ignite by fire, friction, concussion, percussion or detonation of any part thereof which may and is intended to cause an explosion; poisons; carcinogenic materials; caustic chemicals; hallucinogenic substances; illegal materials; drugs that are illegal to sell and/or dispense; and substances which, because of their toxicity, magnification or concentration within biological chains, present a threat to biological life when exposed to the environment, etc.

Soon after the September 11, 2001, terrorist attack on the United States, someone and/or a group of people, has been adding harmful biological agents to the mail. The addition of harmful biological agents to the mail submitted to the USPS has caused the death of some people and necessitated the closure of some post offices and

other government office buildings. Thus, there is an urgent need to exclude life harming materials that are included in the mail.

B. Appellant claims a incoming mail monitoring system that stores unique information that is affixed to mail and the identities of mailers; which has a scanner at a receptacle that reads the unique information before mail is permitted to enter the interior of the receptacle; and, communicating to the recipient information stored in the data center about the mail.

This invention overcomes the disadvantages of the prior art by providing a system that enables recipients of letters, flats and/or packages (hereinafter "mail") that are addressed to a recipient to determine the identity of the person or group that placed an indicia and other information on mail, i.e., the person or group who was issued unique stamps and/or labels by the post. The identity of the mailing would also be uniquely identified. Since the identity of the mailer, the time the mail was placed in a receptacle and the item being mailed in a receptacle would be known, people would not likely place life-harming material in the mail if they would likely be apprehended. Thus, this invention is able to access the likelihood that the mail contains life harming materials before the mail enters the interior of a receptacle, i.e., mailbox. Hence, the carrier may be able to remove mail from the mail stream at its entry point to the mail stream before it causes human harm and/or causes extensive property damage.

This invention accomplishes the foregoing by storing unique information that is affixed to mail and the identities of mailers; having a scanner at a receptacle read the

unique information before mail is permitted to enter the interior of the receptacle; and communicating to the recipient information stored in the data center about the mail.

Claim 1 is the only independent claim in this patent application. Claim 1 relates to an incoming mail monitoring system. Claim 1 includes the following elements one or more data bases that stores unique information contained in a postal indicia affixed to mail and identities of mailers; a plurality of receptacles that reads and stores the unique information affixed to mail after the mail enters the interior of the receptacle; a data center that stores the unique information affixed to mail and receives the unique information from the receptacles to determine if the mailer is permitted to enter mail in the receptacle; and means coupled to the data center and the recipient of the mail for communicating to the recipient, information stored in the data center about the mail.

The foregoing method is shown in Fig. 1 and Fig. 2 paragraph 0021 on page 5 to paragraph 0032 of page 11 of Appellants' Patent Application. A copy of Fig. 1 appears next to this page.

Referring now to the drawings in detail, and more particularly to Fig. 1, the reference character 11 represents an electronic postage meter. Postage meter 11 includes a funds vault 12 that represents the value of the postage that may be used by meter 11; an accounting and encryption module 13 that contains information that is used to print indicia 18; a printer 14; a scanner and processor 15; a controller 16; a clock and calendar 6; a user I/O 17, and an I/O 56. Accounting and encryption module 13 obtains a security code that may be obtained from address field 9 of mail piece 10 and information contained in postage meter 11. The manner in which the aforementioned security code is obtained is disclosed in the Sansone, et al. United

States Patent No. 4,831,555 entitled "Unsecured Postage Applying System" herein incorporated by reference. User I/O 17 comprises a keyboard in which an operator may enter information into meter 11 and a display in which a operator of meter 11 may read information about meter 11. Funds vault 12, accounting and encryption module 13; indicia printer 14; scanner and processor 15; clock and calendar 6; and user I/O 17 are coupled to controller 16. Clock and calendar 6 provides an internal source of time and date for controller 16. Thus, clock and calendar 6 will supply the instant date and time that meter 11 affixed the indicia to mail piece 10. Scanner and processor 15 will store the above information in processed mail data buffer 54 (described in the description of Fig. 3A).

Actions performed by meter 11 are communicated to controller 16. Controller 16 controls the actions of postage meter 11. Clock and calendar 6 also permits controller 16 to store the date and time that postal indicia 18 was affixed to mail piece 10. Controller 16 uses the weighing of the mail piece to determine the correct postage, and causes meter 11 to affix the correct postage to the mail piece. Controller 16 is described in Wu's United States Patent No. 5,272,640 entitled "Automatic Mail-Processing Device With Full Functions" herein incorporated by reference.

The user of meter 11 places the mail piece to be mailed on a scale (not shown) and enters the classification of the material to be mailed, i.e., first class mail, standard mail, parcel post, etc., into the keyboard of user I/O 17, and relevant information regarding the object to be mailed is displayed on the display of user I/O 17.

Printer 14 will print postal indicia 18 on mail piece 10. Scanner and processor 15 scans address field 9 and sender return address field 8 of mail piece 10. Then

scanner and processor 15 segments the information contained in fields 8 and 9 and stores the segmented information, i.e., tracking code 7. Tracking code 7 may be similar to or the same as the security code determined by accounting encryption module 13. For instance, a unique tracking number may be composed by assembling a number that includes the meter number, the date of mailing of the mail piece, the time of day, the postage placed on the mail piece, the zip code of the licensee of the meter, the name, address, city, state and zip code of the sender of the mail piece, and the name address, city, state and zip code of the recipient of the mail piece. It will be obvious to one skilled in the art that any combination of the aforementioned variables may be used if the meter number is included. In the United States, meter manufactures identify their meters by one or two alpha characters before the meter number. It will also be obvious to one skilled in the art that many other variables may be used to produce unique tracking numbers.

I/O 56 is coupled to modem 20 and scanner and processor 15. Modem 23 is coupled to modem 20 via communications path 24, and modem 21 is coupled to modem 23 via communications path 25. Modem 23 is coupled to postage meter manufacturer data center computer 26. Modem 23 is coupled to postal data center 516 via communications path 521. Computer 26 manages the day-to-day operation of its postage meters metering, i.e., installing new postage meters, withdrawing postage meters, and refilling postage meters with customer funds.

Computer 26 is coupled to postal funds data base 27. Data base 27 stores postal funds that have been used and credited to meters 11 and 41. Computer 26 is also coupled to outbound mail data buffer 28 that receives information about mail piece

10 from postage meter 11, i.e., tracking number 7 and address field 9; inbound mail data buffer 29 that receives information about mail piece 10 from postage meter 41, i.e., tracking number 7 and address field 9; mail box entry data buffer 518 that buffers the scanned data from receptacle 500 (Fig. 2); and, upload data computer 30 that receives and processes information from buffers 28 and 29. Processed mail data base 31 is coupled to upload data computer 30. Processed mail data base 31 stores the result of the output of computer 30 and makes it available to computer 26 for transmission to meter 11.

Postage meter 41 includes a funds vault 42 that represents the value of the postage that may be used by meter 41; an accounting and encryption module 43 that contains information that is used to print postal indicium; a printer 44; a scanner and processor 45; a controller 46; a clock and calendar 58 that permits controller 46 to store the date and time that scanner 45 scanned mail piece 10; a user I/O 47; and an I/O 57. Funds vault 42, accounting and encryption module 43, indicia printer 44, scanner and processor 45, and user I/O 47 are coupled to controller 46. I/O 57 is the interface between scanner and processor 45 and modem 21, and is used to upload data from meter 41 to computer 26 via modems 21 and 23. Clock and calendar 58 will supply the instant date and time that scanner 45 reads mail piece 10. The above information will be stored in processed mail data buffer 54 of Fig. 3A.

Thus, meter 41 is the same as meter 11. In this example, meter 41 is being used as the receiving meter, and meter 11 is being used as a sending meter. It will be obvious to those skilled in the art that meter 11 may be a receiving meter and meter 41 a sending meter, and that additional meters may be connected to computer 26.

After indicia 18 is affixed to mail piece 10 by postage meter 11, mail piece 10 is placed in slot 507 (Fig. 2) before it enters control chamber 510 and inner chamber 514 of receptacle 500. Mail deposited in inner chamber 514 of receptacle 500 will subsequently enter USPS mail delivery process 32 (Fig. 1). The description and operation of receptacle 500 is described in the description of Fig. 2. The post delivers mail piece 10 to the owner of electronic postage meter 41. Mail piece 10 will be scanned by scanner and processor 45 of meter 41. Scanner and processor 45 segments the data and stores it for uploading to Postage meter manufacturer data center computer 26 via modems 21 and 23. Information from meter 11 regarding mail piece 10 was previously sent to computer 26 via modems 20 and 23. The information transmitted by meter 11 is tracking number 7, address field 8, and address field 9. The information transmitted by meter 41 is tracking number 7, return address field 8, and address field 9, the date and time mail piece 10 was scanned by meter 41 and the serial number of meter 41.

Fig. 2 is a drawing of mail receptacle 500 of Fig. 1. Receptacle 500 has a front panel 501 containing a slot 508 for receptacle identification cards 600 and 610 (Figs. 11A and 11B, respectively) and a mail slot 507 for depositing mail; a top panel 505; side panels 502; a back panel 503 having a door 504 for access to life-harming materials; and, a door 506 for access to non-life-harming materials. Receptacle 500 has a control chamber 510 that contains a scanner 511 and a transport 512. Card 600 or card 610 is placed in slot 508 and transported by transport 512 to scanner 511 so that scanner 511 may read the information on the card. Then, transport 512 ejects card 600 or card 610 through slot 508. When mail and/or mail piece 10 (Fig. 1) is deposited face up in slot

507, mail piece 10 will enter control chamber 510. The face of mail piece 10 will be scanned and read by scanner 511 while being moved by transport 512. Mail box controller 513 will interpret the foregoing information regarding mail piece 10. Controller 513 will communicate with postal data center 516 Fig. 1) via data buffer and modem 520. Postal data center 516 communicates with computer 26 (Fig. 1) which accesses buffer 29 to determine if a record of the mail currently in control chamber 510 appears in buffer 29.

If the information on the face of the mail piece in control chamber 510 does not match the information in buffer 29, the mail in control chamber 510 is of questionable origin and may be suspected of having life-harming material. The mail will remain in control chamber 510, and a signal will be sent by controller 513 to postal data center 516 (Fig. 1) to inform the proper authorities to unlock door 504, remove the possibly tainted mail, and activate door 519 to close slot 507 to prevent any mail from entering chamber 510. Controller 513 will also activate LED 517, which will indicate "Out Of Service" or "May contain life-harming materials", etc .

If the information on the face of the mail piece in control chamber 510 matches the information in buffer 29, the mail in control chamber 510 is not of questionable origin and is not suspected of having life harming material. The information will be stored in buffer 518 (Fig. 1), and computer 26 will authorize controller 513 to open door 515 and enable transport 512 to move the mail in control chamber 510 to inner chamber 514. Mail piece 10 and the other mail in inner chamber 514 may be removed by opening locked door 506.

VI   GROUNDS OF REJECTION TO BE REVIEWED

A. Whether or not claims 1, 3, 6, 13 and 16 are patentable under 35 USC §102(e) for being anticipated by Alden, U.S. Patent Application publication 2003/0072469.

B. Whether or not claims 2, 14 and 15 are patentable under 35 USC §103(a) over Alden and further in view of Bobrow, et al., (U.S. Patent Application Publication No. 2002/0079371).

C. Whether or not claim 5 is patentable under 35 USC §103(a) over Alden and further in view of Rangan et al., (U.S. Patent Application Publication No. 2003/0072469).

D Whether or not claims 7 – 11 are patentable under 35 U.S.C. §102(e) for being anticipated by Alden, U.S. Patent Application publication 2003/0072469.

E. Whether or not claim 12 is patentable under 35 U.S.C. §102(e) for being anticipated by Alden, U.S. Patent Application publication 2003/0072469.

F. Whether or not claims 17 – 18 are patentable under 35 U.S.C. §103(a) over Alden, and further in view of Ananda (U.S. Patent No.: 6,385,731).

F. Whether or not claim 1 should remain provisionally rejected under the judicially created doctrine of obviousness-type double patenting.

VII   ARGUMENTS

A.   Claims 1, 3, 6, 13 and 16 have been rejected by the Examiner under 35 U.S.C. §102(e) for being anticipated by Alden, U.S. Patent Application Publication 2003/0072469.

The Examiner stated the following in pages 2-3 of the July 12, 2005 Final Rejection: "As per claim 1, Alden discloses an incoming mail monitoring system, said system comprises (abstract); one or more data bases that stores unique information

affixed to mail and identities of mailers (database storing information) (abstract, paragraph 17, fig's. [sic] 3-9); a plurality of receptacles that reads and stores the unique information affixed to mail after the mail enters the interior of the receptacle (storing information) (abstract, paragraph 17, fig's. [sic] 3-9); a data center that stores the unique information affixed to mail and receives the unique information from the receptacles to determine if the mailer is permitted to enter mail in the receptacle (storing information) (abstract, paragraph 17, fig's. [sic] 3-9); and means coupled to the data center and the recipient of the mail for communicating to the recipient, information stored in the data center above the mail (transfer of data) (abstract)."

Alden discloses the following in his abstract:

"In a preferred embodiment, a network-based hardcopy mail scanning system to enable a mail recipient to view virtual images of their mail prior to physically receiving said mail. Unwanted mail from unknown origins can be discarded remotely by the mail recipient prior to actually receiving or touching the hardcopy mail. Thus the mail recipient is insulated from contact with potential letter bombs, biological agents, and chemical agents distributed by terrorists through the US or international postal systems. The process includes a means to digitize an image of hardcopy mail intended for a mail recipient, a database to store the digitized image, a scanning service computer connected to said database. Said scanning service computer and a mail recipient computer are interconnected by a computer network. The scanning service computer communicates images of hardcopy mail (addressed for delivery to the mail recipient) to the mail recipient computer via the computer network. The mail recipient can elect to accept mail for receipt or to reject mail which is then destroyed. By virtually

selecting what mail to accept and discarding the rest, the recipient can discard mail from unknown origins prior to ever physically handling it."

Paragraph 17 of Alden reads as follows:

"**[0017]** **FIG. 3** is a flowchart describing hardcopy mail interception at the home mailbox of the present invention. The present invention provides a mail scan service **49**. In this illustration, the mail scan service is intercepting the intended recipient's **55** mail at his home mail box **47**. The **49** scans (records a digital image) of the mail which it provides electronically over the internet, thereby enabling the intended recipient to virtually view the mail prior to receiving it. Internet communication channel between **49** and **55** is indicated by a dotted line. The **55** elects to accept or to reject each specific mail article. Rejected mail **51** is discarded by the **49** and accepted mail **53** is routed to the user by the **49**. Thus the user of the scanning service receives and personally handles only the mail that he wishes to and discards the unwanted mail without ever having handled it. This reduces potential for exposure to explosives, biological agents, and chemical agents distributed by terrorists."

Alden does not disclose a postal indicia. In fact, in Fig. 9, Alden shows what appears to be a cancelled 34 cents U.S. postage stamp in the upper right hand side of the image of envelope 175. A U.S. postage stamp does not identify the party who placed the stamp on the mail.

Alden does not disclose a postal indicia. In fact, in Fig. 9, Alden shows what appears to be a cancelled 34 cents U.S. postage stamp in the upper right hand side of the image of envelope 175. A U.S. postage stamp does not identify the party who placed the stamp on the mail.

Some of the advantages of Appellant's claimed invention over the invention disclosed by Alden are as follows. Alden obtains a scanned image of the face of mail before the recipient receives the mail. From the scanned image Alden's recipient assumes that the party whose name appears in the space provided for the return address is the party who sent the mail to the recipient. It is possible that terrorists may place the name of a entity known to Alden's recipient in the return address space. Whereas, in Appellant's claimed invention data bases store unique information contained in a postal indicia affixed to mail and identities of mailers so that a plurality of receptacles may read and store the unique information affixed to mail after the mail enters the interior of the receptacle to enable a data center that receives the unique information from the receptacles to determine if the mailer is permitted to enter mail in the receptacle and means coupled to the data center and the recipient of the mail for communicating to the recipient, information stored in the data center about the mail.

The foregoing is possible because a postal indicia positively identifies the sender of the mail, i.e. the person or group who applied for a license to use a postage meter to affix postage indicia to mail for the payment of postage. Thus, a third party data center verifies the identity of the party who affixed the postal indicia to the mail to the recipient. Hence, Appellant's claimed invention provides additional security than that disclosed by Alden.

Hence, Alden does not disclose or anticipate the following elements of claim 1, namely, one or more data bases that stores unique information contained in a postal indicia affixed to mail and identities of mailers. Alden also does not disclose the following elements or claim 1 namely, a plurality of receptacles that reads and stores

the unique information affixed to the mail after the mail enters the interior of the receptacle and a data center that stores the unique information from the receptacles to determine if the mailer is permitted to enter mail in the receptacle.

B. Claims 2, 14 and 15 have been rejected by the Examiner under 35 U.S.C. §103(a) over Alden and further in view of Bobrow, et al., (U.S. Patent Application Publication No. 2002/0079371).

Claims 2 and 14 depend on claim 1 and claim 15 depends on claim 14.

Claim 2 specifies that the means of claim 1 is a telephone; and a voice response unit that is coupled to the telephone and the data center.

Claim 14 specifies, the receptacles, includes the time and date that the mail was deposited in the receptacle.

Claim 15 specifies, the receptacles, includes the location of the receptacle.

The Examiner stated in page 5 of the July 12, 2005 Final Rejection: "Bobrow et al. discloses wherein the means comprises: a telephone; and a voice response unit that is coupled to the telephone and the data center (paragraph 12, fig. 1). It would have been obvious to modify Alden to include a telephone, and a voice response unit that is coupled to the telephone and the data center such as that taught by Bobrow et al. in order communicate [sic] with the data center through voice activated means concerning the incoming mail pieces. As per claim 14, Bobrow et al. further discloses wherein the receptacles includes the **time** and **date** that the mail was deposited in the receptacle (paragraph 133, fig's [sic] 2 & 4)."

Paragraph 12 of Bobrow reads as follows:

> "**[0012]** Despite promises of cross-platform integration (e.g.,
> computer and telephone, computer telephony), there is usually
> little relationship between the data on a personal computer and
> most of the documents and other tools used for communication
> and information exchange that are found around a typical
> individual, office, or family. For example, in a typical home or

office, one might find a telephone, an answering machine (or voicemail system), audio equipment (such as a stereo), a fax machine, a television, a computer and printer, a whiteboard or a chalkboard, and various written notes, lists, calendars, mailings, books, and other documents. Unfortunately, the information in one or more of those repositories is usually tied to that repository. For example, addresses in a written address book are not easily used on a computer e-mail system, unless the user goes to the trouble of manually transferring the relevant information from the address book to the computer."

Paragraph 133 of Bobrow reads as follows:

"[0133] Swipes **1114, 1116,** and **1118** specify the date and time of the event. Swipes **1110, 1112, 1122,** and **1124** serve to annotate the event. The address is set forth in swipes **1120, 1122,** and **1124** – this information can remain part of the annotation or can be extracted by the system as described below. Note that this further information can be displayed in a hierarchical fashion, concealing details until needed. Moreover, in one embodiment of the invention, the entire announcement of **FIG. 11** (or at least an additional portion thereof) is scanned and stored as an image in the database **310 (FIG. 3)** in addition to the information extracted and used as an event annotation as set forth above. This approach has the advantage that additional information in the document (such as the bride's name, for example) is accessible and can be made available, if necessary, even if it is not expected to be needed at the time the key data items are extracted."

Alden discloses the following in paragraph 20:

" Fig. 6 is a flowchart describing hardcopy mail scanning performed by an office mail processing system. Many buildings use internal mailroom personnel to

distribute mail. Through out the building, the present invention can be used at the building level as well. After the postal service **93** delivers mail to office mail processing system **95** the office mail service provides a mail scanning service (digital images of the mail are created). An intended receiver **105** is given access to the digital images via the intranet (indicated with dotted line) which interconnects the **97** computer and the **105** computer. Also over the intranet, the **105** sends elections to accept or reject each mail article to the **97** computer. The office mail processing system then delivers the only the accepted mail to the **105** and discards the rejected mail. Thus the user of the office mail scanning service receives and personally handles only the mail that he wishes to and discards the unwanted mail without ever having handled it. This reduces potential for exposure to explosives, biological agents, and chemical agents distributed by terrorists."

Some of the advantages of Appellants claimed invention over the invention disclosed by Alden and Bobrow are as follows. Alden obtains a scanned image of the face of mail before the recipient receives the mail. From the scanned image Alden's recipient assumes that the party whose name appears in the space provided for the return address is the party who sent the mail to the recipient. It is possible that terrorists may place the name of a entity known to Alden's recipient in the return address space. Whereas, in Appellant's claimed invention data bases store unique information contained in a postal indicia affixed to mail and identities of mailers so that a plurality of receptacles may read and store the unique information affixed to mail after the mail enters the interior of the receptacle, (claim 14 as well as includes the time and date that the mail was deposited in the receptacle) (claim 15 the location of the receptacle) to enable a data center that receives the unique information from the receptacles to determine if the mailer is permitted to enter mail in the receptacle and means (Claim 2 a

telephone; and a voice response unit) coupled to the data center and the recipient of the mail for communicating to the recipient, information stored in the data center about the mail.

The foregoing is possible because a postal indicia positively identifies the sender of the mail, i.e. the person or group who applied for a license to use a postage meter to affix postage indicia to mail for the payment of postage. Thus, a third party data center verifies the identity of the party who affixed the postal indicia to the mail to the recipient. Hence, Appellant's claimed invention provides additional security than that disclosed by Alden.

Notwithstanding the foregoing, in rejecting a claim under 35 U.S.C. §103, the Examiner is charged with the initial burden for providing a factual basis to support the obviousness conclusion. *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967); *in re Lunsford*, 375 F.2d 385, 148 USPQ 721 (CCPA 1966); *in re Freed*, 425 F.2d 785, 165 USPQ 570 (CCPA 1970). The Examiner is also required to explain how and why one having ordinary skill in the art would have been led to modify an applied reference and/or combine applied references to arrive at the claimed invention. *In re Ochiai*, 37 USPQ2d 1127 (Fed. Cir. 1995); **in re Deuel**, *51 F.3d 1552, 34 USPQ 1210 (Fed. Cir. 1995);* **in re Fritch**, 972 F.2d 1260, 23 USPQ 1780 (Fed. Cir. 1992); **Uniroyal, Inc. v. Rudkin-Wiley Corp.**, 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988). In establishing the requisite motivation, it has been consistently held that both the suggestion and reasonable expectation of success must stem from the prior art itself, as a whole. *In re Ochiai*, supra; **in re Vaeck**, *947 F.2d 488, 20 USPQ2d 1438*

(Fed. Cir. 1991); in re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *in re Dow Chemical Co.*, 837 F.2d 469, 5 USPQ2d 1529 (Fed. Cir. 1988).

C.   **Claim 5 has been rejected by the Examiner under 35 U.S.C. §103(a) over Alden and further in view of Rangan et al., (U.S. Patent Application Publication No. 2003/0072469).**

Claim 5 depends on claim 1. In claim 5 the recipient transmits coded information appearing on the mail to the data center.

The Examiner stated in page 6 of the July 12, 2005 Final Rejection:

Alden discloses a mail monitoring system as described above.

Alden does not disclose transmitting coded information. Rangan et. al. discloses transmitting coded information such as that taught by Rangan et. al. in order to hide the true meaning of the information discloses.

.   In addition to the arguments made in above section B please consider the following.

Ragan discloses the following in paragraph 0019.

"In another aspect of the present invention a method for gathering raw data from Internet sites and presenting meta-summarized information from the data to a requesting user is provided, comprising steps of (a) receiving a report request by a report processor at an Internet-connected portal system from a user; (b) matching the request to an individual one of multiple report algorithms stored at the portal system; (c) gathering raw data by a data gathering system operating on the portal system from multiple Internet sites associated with the requesting user; (d) processing the raw data according to the report algorithm

into meta-summarized information defined by the report algorithm; and (e) transmitting the meta-summarized information as a report to a destination associated with the report request. The portal system may further comprise an aggregated-data database in the data repository storing aggregated data retrieved for specific users periodically, and there may be a further step for checking the aggregated-data database for needed data before requiring the data-gathering system to retrieve data from the associated Internet sites. In the instance that the needed data is stored in the aggregated-data database, the preparing the report from the aggregated data."

Ragan gathers raw data from Internet sites and presents meta-summarized information from the data to a requesting user. Ragan does not disclose the ability of a recipient to transmit coded information appearing on mail to the data center.

Appellant's claimed invention utilizes data bases to store unique information contained in a postal indicia affixed to mail and identities of mailers so that a plurality of receptacles may read and store the unique information affixed to mail after the mail enters the interior of the receptacle, to enable a data center that receives the unique information from the receptacles to determine if the mailer is permitted to enter mail in the receptacle and means coupled to the data center and the recipient of the mail for communicating to the recipient, information stored in the data center about the mail and for the recipient to transmit coded information appearing on the mail to the data center.

D. Claims 7-11 have been rejected by the Examiner under 35 U.S.C. §102(e) for being anticipated by Alden, U.S. Patent Application Publication 2003/0072469.

Claim 7 depends on claim 6 which depends on claim 1. Claims 8, 9 and 11 depend on claim 7. Claim 10 depends on claim 9.

Claim 7 adds the following limitation to claims 1 and, locating a scanner in a control chamber of the receptacle..

Claim 8 specifies that the control chamber has a locked door for isolating suspect mail.

Claim 9 specifies that the interior of the receptacle comprises: an inner chamber that receives mail from the control chamber that is not suspected of having life harming material.

Claim 10 specifies that the inner chamber has a locked door in which when open mail may be removed from the inner chamber.

Claim 11 includes a slot for depositing mail into the control chamber.

The Examiner stated in page 4 of the July 12, 2005 Final Rejection:

As per claim 7, Alden discloses wherein the scanner is located in a control chamber (scanner in a chamber (holder) (abstract, paragraph 17, fig's 3-9).

As per claim 8, Alden discloses wherein the control chamber has a locked door for isolating suspect mail (separating mail (package, paper) (abstract, paragraph 17, fig's 3-9).

As per claim 9, Alden discloses an inner chamber that receives mail from the control chamber that is not suspected of having life-harming material (separating mail(package, paper) (abstract, paragraph 17, fig's 3-9).

As per claim 10, Alden discloses wherein the inner chamber has a locked door in which when open mail may be removed from the inner chamber (removing mail (package, paper) after it's been separated) (abstract, paragraph 17, fig's 3-9).

As per claim 11, Alden discloses a slot for depositing mail into the control chamber (abstract, paragraph 17, fig's 3-9).

Paragraph 17 of Alden reads as follows:

"FIG. 3 is a flowchart describing hardcopy mail interception at the home mailbox of the present invention. The present invention provides a mail scan service 49. In this illustration, the mail scan service is intercepting the intended recipient's 55 mail at his home mail box 47. The 49 scans (records a digital image) of the mail which it provides electronically over the internet, thereby enabling the intended recipient to virtually view the mail prior to receiving it. Internet communication channel between 49 and 55 is indicated by a dotted line. The 55 elects to accept or to reject each specific mail article. Rejected mail 51 is discarded by the 49 and accepted mail 53 is routed to the user by the 49. Thus the user of the scanning service receives and personally handles only the mail that he wishes to and discards the unwanted mail without ever having handled it. This reduces potential for exposure to explosives, biological agents, and chemical agents distributed by terrorists."

:

Alden's abstract reads as follows:

"In a preferred embodiment, a network-based hardcopy mail scanning system to enable a mail recipient to view virtual images of their mail prior to physically receiving said mail. Unwanted mail from unknown origins can be discarded remotely by the mail recipient prior to actually receiving or touching the hardcopy mail.

Thus the mail recipient is insulated from contact with potential letter bombs, biological agents, and chemical agents distributed by terrorists through the US or international postal systems. The process includes a means to digitize an image of hardcopy mail intended for a mail recipient, a database to store the digitized image, a scanning service computer connected to said database. Said scanning service computer and a mail recipient computer are interconnected by a computer network. The scanning service computer communicates images of hardcopy mail (addressed for delivery to the mail recipient to the mail recipient computer via the computer network. The mail recipient can elect to accept mail for receipt or to reject mail which is then destroyed. By virtually selecting what mail to accept and discarding the rest, the recipient can discard mail from unknown origins prior to ever physically handling it."

In addition to the arguments made in above section A please consider the following.

Alden discloses a mail scanner that reads the face of mail in which rejected mail 51 is discarded and accepted mail 53 is routed to the user. Alden does not disclose or anticipate a receptacle that has a control chamber and a inner chamber, wherein the control chamber may be locked to isolate mail that is suspected of having life harming material.

E.   Claim 12 has been rejected by the Examiner under 35 U.S.C. §102(e) for being anticipated by Alden, U.S. Patent Application Publication 2003/0072469.

Claim 12 depends on claim 11 and claim 11depends on claim 7, which depends on claim 1.

Claim 12 adds the following limitation to claim 11, namely, means for closing the slot when the mail in the control chamber is suspected of containing life harming substances.

The Examiner stated in page 4 of the July 12, 2005 Final Rejection:

As per claim 12, Alden discloses closing the slot when the mail in the control chamber is suspected of containing life harming substances (separating mail (package, paper) (abstract, paragraph 17, fig's 3-9).

In addition to the arguments made in above Sections A and D please consider the following. Alden discards mail that is not accepted. Alden does not disclose any means for closing a slot when the mail in the control chamber is suspected of containing life harming substances. Furthermore, Alden does not disclose the concept of isolating suspect mail. One of the advantages of isolating suspect mail is that the mail may be prevented from entering the mail stream and/or the proper authorities may safely dispose of the suspect mail. Also the proper authorities may want to use the mail to determine the sender and use the mail as evidence in some future proceeding.

F. Claims 17 and 18 have been rejected by the Examiner under 35 U.S.C. §103(a) over Alden, and further in view of Ananda (U.S. Patent No.: 6,385,731).

Claim 17 is dependent on claim 1 and claim 18 is dependent on claim 17. In Claim 17 the unique information is a security code. In claim 18 the security code comprises an address of the recipient of the mail and information contained in a postage meter that made the postal indicia.

The Examiner stated in pages 6 and 7 of the July 12, 2005 Final Rejection the following:

> "Alden discloses a mail monitoring system as described above.
> Alden does not disclose postal indicia containing a security code or
> security code being obtained from a recipient address field on the
> mail and information contained in a postage meter that affixed the

postal indicia to the mail. Ananda discloses postal indicia containing a security code (col.21,27-45 & 52-67; col.22, 45-60; cöl.27, 65-67; col.28, 1-7) and security code being obtained from a recipient address field on the mail and information contained in a postage meter that affixed the postal indicia to the mail (col.21, 27-45 & 52-67; .col.22, 45-60; çol.27, 65-67; col.28, 1-7). It would have been obvious to modify Alden to include postal indicia containing a security code or security code being obtained from a recipient address field on the mail and information contained in a postage meter that affixed the postal indicia to the mail such as that taught by Ananda in order to categorize each peace of mail according to the information that corresponds to each peace of mail and have the security pieces within the system such that the system user can recognize if a piece of mail is secure by analyzing the data on the envelope of the mail."

In addition to the arguments made in above Section A, please consider the following. Ananda discloses the following in lines 27 – 67 of Col. 21.

"The present invention can be applied to secure on-line postage metering service, particularly in conjunction with the United States Postal System (USPS). Currently, meter fraud due to the unauthorized and fraudulent uses of traditional mechanical postage meters is on the rise and a more secure postage metering system is needed to curb meter fraud. Electronic postage meters provide advantages over the traditional mechanical postage meters due to their connectivity and speed. However, an electronic postage metering system requires proper security and authentication methods to successfully deliver secure postage metering services. In this application, the rental software is an on-line postage metering program and on-line dynamic password verification methods described above are used to provide a secure authentication process. The goal of such an electronic postage metering system is to allow a user to print a postal indiciurn at home, at office, or any other desired place by using a printer and a (personal) computer connected to a server in a secure and fraud-free manner. To implement a secure on-line electronic metering system, the invention requires computers equipped with a modem. FIG. 12 shows a hardware block diagram of a secure electronic metering system constructed according to the invention. For discussion purposes, a customer of an on-line postage metering service is referred to as a user or a client. In FIG. 12, user system 1200 functions as an on-line electronic postage meter and comprises a personal computer (PC) 1201, a modem 1202 connected to PC 1201, and a printer 1203 connected to PC 1201.

Modem 1202 is connected to Postal Security Device (PSD) vendor system 1210. As for software requirements, the system shown in FIG. 12 requires on-line postage metering software to provide the on-line postage metering service. In one embodiment of the invention, PC 1201 contains the header code portion of the on-line postage metering program. The header code by itself is not complete and requires inputs from the controller code of on-line postage metering program to be operational. A user or a client must have access to user system 1200 to provide inputs such as desired postage amount, delivery point information, or personal information to the secure on-line electronic metering system."

Ananda discloses the following in lines 45 - 60 of Col. 22.

"Database 1213 comprises system usage log to log every postage metering transaction, quality assurance information for indicium quality assurance purposes, encryption information for user's public key, and user's financial information such as credit cards, user's banking institutions, electronic funds transfer information, and automated clearinghouse transfer information."

Ananda discloses the following in line 65 of Col. 27 to line 7 of col. 28.

"Thus, one embodiment of the invention applicable for electronic postage metering has been described. In alternate embodiments, however, the invention can be used for other secure on-line printing applications. For example, the secure on-line printing system can have a server generate images of checks, tickets, coupons or certificates and transmit them to a user computer for printing on a user printer. Therefore, the invention can be applied to print symbols other than postal indicia in a secure, authenticated manner."

Ananda discloses a secure on-line postage system. Neither Alden or Ananda taken separately or together disclose or anticipate a disclose or anticipate a plurality of mailers' units that stores unique information contained in a postal indicia having a security code affixed to mail; a plurality of receptacles that reads and stores the unique

information contained in the postal indicia before the mail enters the interior of the receptacle.

H.   Claim 1 has been provisionally rejected by the Examiner under the judicially created doctrine of obviousness-type double patenting

The Examiner stated in pages 7 and 8 of the July 12, 2005 Final Rejection the following:

Claim 1 is provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-7 of copending Application No. 09/683380 and over claims 1-8 of copending Application 09/683381. Although the conflicting claims are not identical, they are not patentably distinct from each other because all three disclose a mail monitoring system, said system comprises:
a data base that stores unique information affixed to mail; a plurality of receptacles that reads and stores the unique information
contained in the postal indicia before the mail enters the interior of the receptacle; and
a data center that receives information stored by the mailers' units and the receptacles to identify the mailer and assess the possibility of the presence of life-harming material in the mail..
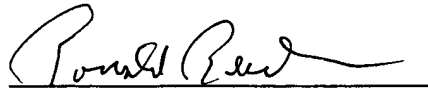
A Terminal Disclaimer was filed in Application No.10/015469 on May 13, 2005 to overcome the double patenting rejection. A copy of the Terminal Disclaimer is attached hereto in Section XI.

In view of the above Appellants respectfully submit that appealed claims 1 - 18 in this application are patentable. It is requested that the Board of Appeal overrule the Examiner and direct allowance of the rejected claims.

Respectfully submitted,

Ronald Reichman
Reg. No. 26,796
Attorney of Record
Telephone (203) 924-3854

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

What is claimed is:

1. An incoming mail monitoring system, said system comprises:

one or more data bases that stores unique information contained in a postal indicia affixed to mail and identities of mailers ;

a plurality of receptacles that reads and stores the unique information affixed to mail after the mail enters the interior of the receptacle;

a data center that stores the unique information affixed to mail and receives the unique information from the receptacles to determine if the mailer is permitted to enter mail in the receptacle; and

means coupled to the data center and the recipient of the mail for communicating to the recipient, information stored in the data center about the mail.

2. The system claimed in claim 1, wherein the means comprises:

a telephone; and

a voice response unit that is coupled to the telephone and the data center.

3. The system claimed in claim 1, wherein the means comprises:

a computer coupled to the data center via the Internet.

4. The system claimed in claim 1, wherein the recipient transmits recipient and mailer name and address information appearing on the mail to the data center.

5. The system claimed in claim 1, wherein the recipient transmits coded information appearing on the mail to the data center.

6. The system claimed in claim 1, wherein the receptacle units include a scanner that reads the mail.

7. The system claimed in claim 6, wherein the scanner is located in a control chamber.

8. The system claimed in claim 7, wherein the control chamber has a locked door for isolating suspect mail.

9. The system claimed in claim 7, wherein the interior of the receptacle comprises: an inner chamber that receives mail from the control chamber that is not suspected of having life- harming material.

10. The system claimed in claim 9, wherein the inner chamber has a locked door in which when open mail may be removed from the inner chamber.

11. The system claimed in claim 7, further including a slot for depositing mail into the control chamber.

12. The system claimed in claim 11, further including means for closing the slot when the mail in the control chamber is suspected of containing life harming substances.

13. The system claimed in claim 12, further comprising means for indicating a message indicating the status of the receptacle.

14. The system claimed in claim 1, wherein the receptacles includes the time and date that the mail was deposited in the receptacle.

15. The system claimed in claim 14, wherein the receptacles, includes the location of the receptacle.

16. The system claimed in claim 1, wherein the receptacle unit includes: means for informing the post of possibility of the presence of life harming material in the mail.
17. The system claimed in claim 1, wherein the unique information is a security code.

18. The system claimed in claim 17, wherein the security code comprises an address of the recipient of the mail and information contained in a postage meter that made the postal indicia.

IX EVIDENCE APPENDIX

There is no additional evidence to submit.

X RELATED PROCEEDING APPENDIX

a) U.S. Patent Application Serial No. 10/015,464 entitled "Method And System For Accepting Non-Harming Mail At A Home Or Office" is presently on appeal to the Board Of Appeals

b) U.S. Patent Application Serial No. 10/015,309 entitled "System For Receiving Non-Harming Mail At A Receptacle" is presently on appeal to the Board Of Appeals

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on December 6, 2005
Date of Deposit

Amy Harvey
Name of Rep.

Signature

December 6, 2005
Date

XI TERMINAL DISCLAIMER

CORRECTED   DEC 0 8 2005   CORRECTED

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION	Docket Number (Optional) F-435

In re Application of: Ronald P. Sansone

Application No.: 10/015,469

Filed: December 12, 2001

For: SYSTEM FOR A RECIPIENT TO DETERMINE WHETHER OR NOT THEY RECEIVED NON-LIFE-HARMING MATERIALS

The owner*, __Pitney Bowes Inc._____, of __100__ percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number __10/15309 & 10/015464__, filed on __December 12, 2001 /*__, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. _26,796_____

_____   _5/11/05_____
Signature   Date

RONALD REICHMAN
Typed or printed name

_203-924-3854_____
Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is ~~included~~. to be charged to deposit account 16-1885;

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*and 09/683380 and 09/683381, both filed December 19, 2001,

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this statement. See MPEP § 324.